(2)

PERSPECTIVES ON TRUSTED COMPUTER SYSTEMS

Willis H. Ware

September 1988

P-7478

The RAND Corporation, 1700 Main Street, P.O. Box 2138, Santa Monica, CA 90406-2138

PERSPECTIVES ON TRUSTED COMPUTER SYSTEMS[1]

INTRODUCTION

The topic of this paper is trusted computer systems and their place in the world, as well as their contribution to the overall cause of computer security. First, however, there are some background aspects to deal with, so that it is clear what the issues are and what the specialized terminology means.

Since the concept of "trusted systems" originated in the United States, the general context of the following discussion is the historical evolution of the computer security issue there.

REVIEW OF HISTORY

Let's review the history to understand where we are in computer security and how we have arrived at the present position.

Computer security was first introduced publicly in the United States at the 1967 spring meeting of the National Joint Computer Conference in Atlantic City, N.J.[2] At the time, the NJCC-sponsored meetings were the biggest computer-related technical meetings each year. A special group of papers had been organized to introduce the topic of computer security to public discussion. Although security controls in computer systems had been a subject of interest in the U.S. defense establishment, computer practitioners and owners of systems in the commercial world and in civil government had really not heard about it.

Soon afterward the United States government organized an advisory group to assist it in establishing appropriate policy guidance. The study conducted by the group became the well-known (at least in the

[1] Presented as keynote speech at IFIP/SEC'88 Conference, Conrad International Hotel, Gold Coast, Queensland, Australia, May 20, 1988. To be published in the conference proceedings by Elsevier Advanced Technology Publications, Oxford, England.

[2] "Security and Privacy in Computer Systems," *AFIPS Conference Proceedings*, Vol. 30, 1967, pp. 279-300.

United States) "Defense Science Board study," named after the sponsoring body. The final report was published in 1970 and is sometimes referred to as "the Ware report." It has been generally available outside the defense establishment since 1979.[3]

The motivation for the DSB Study was the emergence of time-sharing computer systems and their alliance with communications, plus the fact that the government did not have at the time an adequate policy for such systems.

The members of the group that did the work all came from the defense establishment if they were from government; or if not in government, they knew defense intimately. The commercial user world simply was not represented. The focus of the effort, therefore, was any computer system that had to control access to defense classified information.

There was an early recognition--perceived at the time as essential--that computer people, no matter how much they would prefer it, would never be able to force a restructuring of the defense classified scene as it had developed in a paper-oriented world. Moreover, there was the accompanying realization that they should not even try. There was also recognition that a lot of people from the paper world would have to transfer to, work in, and feel comfortable with the computer world. Whatever could be done to ease the transition would be desirable. Hence, the DSB Committee made a fundamental initial decision to structure the security controls within the computer in the image of the paper world.

Parenthetically, I think the same observation is still true, and perhaps more so. The easier the computer professionals of the world make the transition from older ways of conducting business to the newer computer-based ways, the better received we and our systems will be and the more powerful will be our voices on important issues.

---

[3]Willis H. Ware (ed.), *Security Controls for Computer Systems*, Report of the Defense Science Board Task Force on Computer Security, published for the Office of the Secretary of Defense by The RAND Corporation, Santa Monica, California, as a classified document February 1970; reissued by RAND as an unclassified publication R-609-1, October 1979.

In the defense paper world, the essential issue always has been that of controlling the access of individuals to information. In doing so, there have been rudimentary audit trails in the form of logs and access lists, but there are no analogs of automated processes working in behalf of a user, or automated processing of the information within a document. Thus, it is not surprising that the DSB report addressed only access control as the central issue.

DEVELOPMENT OF THE 1970s

Funded Efforts

The DSB activity led to a sequence of things. Through the early and mid 1970s, the defense community wrote and rewrote policy documents. Two agencies of the United States government--the Advanced Research Projects Agency (now DARPA) and the United States Air Force--kept the subject alive technically. They funded deliberate penetration efforts, partly to support policy positions that the government needed to take, and partly to persuade organizations that computer systems were in fact vulnerable to outside penetrations.

The research work focussed predominantly on system specification and evaluation. There were several invitational workshops, but the common thread through everything was the software issue and, in particular, the operating system aspect. Emphasis on software, of course, was crucial since it was the dimension of the problem that at that point in time had received least attention.

Defense Activity

In 1977, the defense establishment began a so-called Computer Security Initiative to focus attention and action on the issue. In response to it, there were additional workshops during 1977 and 1978 addressing various aspects of secure systems, and the first of the Federal Standards for computer security appeared.

The concept of a "trusted system" appeared along the way. We will return later to a discussion of the word "trust" and its implications; but for the moment, basically trust implies that something can be depended on to do a specified job with high confidence

By the end of the decade, there was a good awareness of what it would mean to design a secure operating system for a mainframe computer, and there was a modest body of research achievements on which to build. Preliminary concepts for evaluating systems and a number of relevant technical concepts had developed.

Commercial Activity

Concurrently in the commercial world, there was little activity other than a very slowly growing awareness that computer security indeed was a real thing, not something invented by the computer people to sell more equipment and software. Vendors preferred not to raise the subject lest customers conclude that computers were risky devices that were not dependable. Such a view would naturally inhibit sales. There was a small amount of educational and guidance material available from a few sources, but not much.

Related Activity

Also of importance in the 1970s were certain activities in the nondefense U.S. government, notably various ones related to personal or informational privacy. A cabinet official (Secretary Elliot Richardson of the Department of Health, Education, and Welfare) sponsored the Advisory Committee on Automated Personal Data Systems which reported in 1973. Its report, also sometimes called "the Ware report," became the intellectual foundation for the Federal Privacy Act of 1974 which is the most comprehensive of United States privacy laws. It in turn created the Privacy Protection Study Commission which reported to President Carter and the Congress in 1977.

These events called attention to the need for protecting personal information and for controlling access to it. Thus the attention to privacy spurred attention to computer security in parts of government that previously had ignored it.

INTO THE 1980s

By the 1980s, we, the computer specialists in security, understood that building an operating system which could enfore security safeguards was a very difficult job technically and an expensive one. We also had general agreement that it would require redoing commercial products; security controls could not be satisfactorily retrofitted.

At the time, the government was moving more and more into systems that demanded security control, and the big question became:

- How would the U.S. government get secure software products?

An imaginative person[4] decided that a deal could be arranged. If industry could be persuaded to invest its funds in designing and implementing secure software products, the government would test and certify them at no charge. Hence, industry would have the proper products to supply for government needs.

The idea looked like a winner all around. Industry would underwrite the cost for the software development; the government had the expertise (it believed) to test the software and would get products that it needed. A side payoff was that industry would have secure software systems for other customers as well.

However, a focal point within government was clearly necessary to oversee the activity.

The National Center

There was considerable debate about the issue, but ultimately it was agreed that a technical center would be established at the National Security Agency which would become the executive agent for the center and for computer security in behalf of the government. From the beginning, the concern was for a center that could service all of government, but it apparently never occurred to anyone that the security

[4]Stephen T. Walker, then of the Office of the Under Secretary of Defense for Research and Engineering, Department of Defense, and now president of Trusted Information Systems, Inc., Glenwood, Maryland.

problems of defense and civil government might be different in detail, not just in magnitude.

The Computer Security Evaluation Center (CSEC) was formed in January 1981 to assist the government with regard to computer security. In brief, it was to conduct evaluations of computer systems with regard to security, to set standards for them, and to conduct R&D in behalf of the related technical issues.

The stage had been set for the creation of (what people refer to as) the "colored literature."

The Orange Book[5]

The Orange Book was about to be born from the groundwork that had been laid through the 1970s. The Criteria and its concepts and approach to computer security have been briefed widely, including Australia, so there is a general awareness of its details and its implications in many places.

The Orange Book was the first effort to structure a comprehensive set of evaluation criteria for computer systems that enforce security controls, admittedly a complex job. It has to be seen as a very good but nonetheless first cut at specifying the attributes of computer systems that incorporate security safeguards.

The influence of the Criteria on the vendor community has been significant, and today we are beginning to see products which meet the requirements set forth in the Orange Book and which provide specified security safeguards that function with high confidence.

---

[5]So-named because of the color of its cover. Its full and proper title is *Department of Defense Trusted Computer System Evaluation Criteria*, DoD Computer Security Center (now the National Computer Security Center), CSC-STD-001-83, 15 August 1983. The phrase "Orange Book" is a widely used and accepted substitute phrase for the formal title.

HERE IS TODAY

Here we are today. The CSEC, now called the National Computer Security Center, is a little over seven years old and the Orange Book about four years old. The point of this summary of history is to emphasize that the computer security issue in the United States has developed solely from a defense ancestry. All the progress has been driven by the needs of the defense establishment, something that has been true from the first study onward until today. Moreover, the orientation is the part of the defense community in the United States that deals with classified information. Hence, it is not surprising that the Center's views, policies, actions, and guidance reflect such a lineage.

Consequently, one would expect that the Center's response and actions would automatically be to implement the standing requirements of the defense community for protecting and controlling access to a country's secrets. The Center was bound to see the threat against computer systems as the traditional one that prevails in a defense community anywhere, namely the unfriendly opponent who can mount a persistent, technologically advanced, well-financed ongoing attempt to penetrate systems.

THE WORD *TRUST*

The next order of business is to define the very special word *trust*. Recall that it originated in the 1970s with a group that had been studying primarily software issues and debating how computer systems should be evaluated for security strength. Initially it was a concept to describe a computer system that (1) would include security safeguards and (2) could enforce control over access (a) to the information in it, (b) to the processes in it, and (c) to the resources within it (e.g., memory space, disk space, I/O capability, processing power).

More precisely, the term *trust* meant a system that could enforce a security policy with extremely high confidence. One must immediately note that a *security policy* is the set of rules governing who may access

what information, and what each may do with it, and who may access processes and system resources. The prevailing notion throughout has been, however, that control of access would be central to any security policy.

High confidence relates to the certainty with which a system owner and the accreditor[6] hold a conviction that the security features function as expected, and are themselves protected against inadvertent or deliberate modification. There is a collateral implication that the security features do indeed implement the intended security policy--the access control rules.

Finally, there is also the notion of *integrity* which in this context relates to the ongoing assurance that the protection features continue to be what they are expected to be.

Trust as a Broad Concept

The appearance of the Orange Book caused the word *trust* to take on a narrower meaning. To some extent the title and certainly the contents of the document allied the word *trust* with software. So today the common usage of trust is in the context of system software or major components of it, and the phrase *trusted computing base* is generally a reference to the software components of a system.

In the back of people's minds, of course, is the broader meaning, but the popular discussion is in terms of software. Trust is little used for hardware; it is sometimes used for systems, but even then it conveys a software connotation.

In fact, trust is a very useful concept but it should not be confined to software. It properly can and should be applied to hardware/software combinations; to communication networks; to overall systems; to application programs; to individual components of a system; to information processes whether automated, manual, or both; to procedures whether automated or manual; and, particularly, it should be

[6]The authority who authorizes a system to commence operations after reviewing the threat against a system, the safeguards within it, and the operational need for it. In effect, the authority accepts any residual risk of operating the system.

applied to people. Of course, there are other dimensions of systems such as integrity and reliability that have an impact on the security strength of a system and contribute to it.

Wherever used--be it to the overall system, to components, to software, hardware, processes--trust implies two things:

- The security functions that a system provides do indeed exist and function with high confidence (referred to as the *security features* incorporated on the system); and
- Specific and explicit steps have been taken to assure the confidence and, indeed, to estimate it (called the *assurance measures* for the trusted system).

Trust and People

Let's not miss an important observation. People must be seen as a trusted component in many, possibly most, circumstances. In fact, people that are a part of an information process must be seen as a trusted component of the process if it is to be a trusted one. In addition, if people are a part of a path along which information can or might move, they must also be regarded as a trusted component if the path is to be a trusted one. People as an aspect of trustedness are generally not so identified, and even less talked about.

In addition, it is unfortunate that we cannot and do not know how to measure trustedness of people very well. It is possible to make field investigations. People can be bonded; we can take out insurance against their misbehavior. Often, though, system designers try to offset the inability to measure personal trust with security measures--sometimes procedural, sometimes administrative, sometimes technical, sometimes all such things.

Trust in a Larger Context

There is anotner aspect of trust to be noted. Vendors will offer trusted operating systems, and/or major components of them, and/or major additions to them; and the federal government in the United States will test and certify them. Sometimes a complete hardware/software combination will be certified.

But there are critical other aspects of trustedness that will necessarily be the responsibility of the using organization. Some of them are the following:

- Applications software--does it do what it is supposed to do with high confidence? Have assurance measures been taken to estimate or measure or to quantify the confidence?
- Operational procedures--do they support other security safeguards? Do they substitute for other security safeguards that we do not know how to implement? Or are too expensive? Do they function with high confidence? These questions go beyond the usual acceptance testing of software and the operational testing of it.
- People--have we done our best to establish their trustedness wherever it is essential? Have we implemented technical/procedural/ management safeguards to buffer us against malfeasance of individuals?

The discussion need not be extended further. We must only remember that there are many dimensions of computer security, and that all must be attended to. They are:

Physical security--which is the first thing that everybody learned to do
Personnel security
Administrative security
Procedural security
Management oversight
Hardware security
Software security
Communications security

Every one of them has to be considered individually and in combination in the light a requirement for trustedness and trusted behavior.

To emphasize the point differently, trusted software (important as it is) even though evaluated and certified to meet certain criteria, does not assure an overall operational trusted system. In fact, in some

circumstances, it may well be that other dimensions of computer security can perfectly well provide the needed level of protection and, therefore, assure the necessary degree of system trust.

THREAT

Next, think about threat. Given the ancestry of the Orange Book, the criteria that it contains, and indeed the entire computer security thrust as it developed in the United States, it is not surprising that the threat implicitly addressed by guidance from the National Center would be that associated generally with a defense environment.

Defense Threat

One would expect that the National Center's actions would automatically be to implement the standing requirements of the national security community for protecting and controlling access to the country's secrets--particularly those secrets which relate to the country's ability to counter, offset, circumvent or parry unpleasant things that an unfriendly opponent can do to it. The National Center was bound to see the threat against computer systems as the traditional one that prevails in a defense community--a threat from a well-funded, sophisticated, experienced, and persistent opponent. After all, the defense community in any country has accumulated centuries of experience with unfriendly opponents and the ways of espionage.

Defense Support Systems

There are clearly other parts of a defense establishment for which the threat is somewhat different; namely, the so-called support systems which include the logistic supply to military services, personnel services which basically distribute entitlements of various sorts, financial services, food services, or medical services. Such systems normally deal with unclassified information not usually of particular interest to an opponent, although some of them handle sensitive personal information (e.g., medical records).

For the support side of defense--as opposed to the operational and intelligences aspects--the peacetime threat is not an unfriendly opponent. The threat arises from within, users or system people who decide to misuse (rip off, in common parlance) a computer system for personal gain. The threat is that of the insider who commits some aspect of fraud, embezzlement, waste, theft or abuse, with the foreign opponent in a distant second place. During wartime, of course, the foreign opponent increases in importance.

Threat Differences

Examine the two kinds of threats from a different point of view. The traditional threat from a foreign opponent is technically sophisticated, well-funded, intense, long-standing, persistent, focussed, and very explicitly targeted to acquire specific kinds and items of information from computer systems. The second, the insider threat, is none of these but is an opportunistic one with possible overtones of focusing or targeting. The insider threat is generally unsophisticated technically, and is often an isolated or limited occurrence. Moreover, the intent often is not to steal information from the system, but rather to exploit the system weaknesses for some valuable resource such as funds, or warehouse inventory, or even just computer time.

The second threat reflects the unauthorized actions of the authorized system user; the threat is from one's own side--our person, not theirs. In the military context, of course, things can change during wartime when personnel details, logistics movements, and a lot of other things can be of tactical value to an opponent, but during peacetime there are important differences in security requirements between the classified and unclassified systems of a defense environment.

Business and Industrial Threat

The insider threat against the computer systems and networks of the business and industrial sector is like the second, not the first--at least as evidenced by the incidents we know about, the data we have been able to collect, and the views of the people concerned with the issue. Some day, when the business and commercial sector successfully counters its insider threat, there may be an evolution toward a more sophisticated variety; but such an event is downstream, probably a decade or more away.

Threat Contrast

At the outset in the early 1980s, the dominant requirement in the U.S. Federal government was to provide computer systems that could withstand the defense threat of the foreign opponent. All the actions of the Federal government supported such a view: the positioning of the National Center, the explicit signals to the vendor community, the policy statements, and even the speeches and presentations by officials of the defense establishment.

But what we can see clearly now, discuss in retrospect, and put in perspective was not clear in the early 1980s. Probably no one at the time reflected on two central issues:

- Is the threat against the computer systems of civil government the same as that against defense government? Moreover, does the threat against the computer systems of the private sector resemble any of the threats against government systems?
- Are the safeguards needed to combat the in-government defense threat the same ones that civil government will need? Are they the same ones that the private sector will need?

There is now a growing understanding that such questions are pivotal and must be addressed. It is appreciated that the threat in the private sector does indeed have some very important attributes which differ from that of defense government.

TRUSTED PEOPLE

A particular item of concern in providing trusted systems for any threat will be the people within the systems--the operators, maintainers, designers--and the people which the system serves, the end users. Remember what we will have to do in a trusted system:

- Implement trusted processes, which implies that the proper things must happen to the proper data under the control of and subject to the actions of the proper people--all with extremely high confidence.

Such a statement implies that (1) we must place trust in many individuals who will be in different parts of the system; and (2) in the design of trusted processes which operate with trusted paths, people must be explicitly considered as a component of the path and process.

Defense Environment

In the defense environment, it is accepted doctrine that the discipline of being in the military service plus the shadow of military justice in the background will assure:

- Trusted behavior by people.

Often a defense organization backs up this doctrine, particularly for its civilian employees, by going through formal investigative processes of people's backgrounds, behavior, lifestyle, financial circumstances, etc.

- It is a process of establishing the level of trust that can be attached to an individual. This measurement is reflected in terms of a so-called clearance which is a prerequisite for being allowed access to specified kinds of defense information.

How well this works, how effective it is, and other details are not pertinent to this discussion. But what is very relevant is the observation that similar restraints on behavior do not exist in the private sector.

Private Sector

Business and industry are constrained by social mores, by cultural attitudes, and even by law against being nosey about just those details of an employee's background that are most pertinent to assessing trust; or to making the equivalent judgment of the likelihood that a person will breech the trust implicitly or explicitly vested in him.

The consequence of such an observation is quite straightforward. The measures and safeguards that collectively provide the computer security protection must be designed to counter the unmeasured, and therefore uncertain, levels of trust of some, or perhaps all, individuals within and served by a system.

This is a new dimension for the computer security practitioner. He now must think beyond just the control of access to information, processes, and resources in a system. He must now imagine security safeguards that can be effective against individuals somewhere in the system--but which ones he will not know--that behave in an untrusted manner--but again he will not know how or what they might do.

WHAT CAN WE SAY RETROSPECTIVELY?

With history and background behind us, we can now search for conclusions about computer security. At best some twenty years old as a professional field, the really active phase of computer security practice is only about ten years old. The organized major defense thrust in the United States is eight years old, and the guidance and policy from the National Center only five years old.

What perspectives are there at this point? What has been learned? What can be said about the future? How does trusted software, constructed according to Orange Book precepts, fit into the overall scheme of things?

Perspectives

The first response, by this time, is almost automatic.

- The private sector threat differs from the defense threat in very significant ways. Indeed, there appear to be defense systems whose threat more resembles that of the private sector than other parts of the defense sector.

There are several others:

- With regard to security safeguards, if we assume that the guidance and precepts of the National Center are pertinent and relevant to the defense threat, it remains to be shown that the safeguards recommended against defense threats can accommodate the commercial threat.
- Clearly, some of the Orange Book safeguards are pertinent and relevant (e.g., user logging and user authentication). It is not yet clear that the Orange Book safeguards are a sufficient set to implement all the controls that the commercial world will require.

  Such an observation is neither critical nor negative, but rather a comment as the mathematician would make it. The case simply has not been demonstrated because the experience has not been accumulated nor some of the basic studies completed. Therefore, the question must remain open and unanswered at the present.
- It is certainly clear that the response from vendors and the details of federal policy have both been driven by the ancestral threat of the unfriendly opponent. It has not been driven by the insider threat. Furthermore, since the federal government has been the "only ballgame in town," naturally the vendors have responded to it.

- A national/international aspect has become apparent. While defense communities cooperate across national lines, private corporations exist and operate in many and differing national jurisdictions. For example, it is important to any international organization that it be allowed to take security products freely across national boundaries.

  From the view of the vendor of secure computer systems or just of security products, it is extremely important that he be allowed to sell his products worldwide. Turned around, this point implies that the design of a secure system would ideally be readily and economically convertible from a configuration that can satisfy in-country defense needs to a configuration that is exportable and can satisfy international corporate needs. Many products of commerce exist in domestic and export versions. We must learn how to do the same thing with secure computer systems and trusted products.

Significant Differences

We can now appreciate that some things are important to the defense community that are unimportant or even undesired in the private sector.

- In the defense world, information has to be carefully and completely labeled in order to control access to it with adequate granularity. Data of differing sensitivities are likely to be commingled in the same computer system.

  But in the private sector, whole bodies of data are often separated on the basis of sensitivity (e.g., payroll records, medical histories) and only a little high labeling is required.

- In the defense environment, cost is important but not dominant. Moreover, the defense world cannot really measure the cost of losing information and, therefore, it is hard put to do a cost-vs-security versus expected-loss analysis.

On the other hand, the commercial world can very often measure loss (e.g., goods pilfered, funds embezzled). To the private sector, cost of security will be an important issue.

- The private sector turns over its computer hardware, and sometimes software, very frequently on the basis of cost-performance improvements; the defense sector turns over its installations about half as frequently.

  Therefore, the time to test and certify a product versus its expected market lifetime is important to the vendor, and the time-to-certify versus turnover-cycle-time is important to the private installation.
- The impact of security controls on the throughput performance of a system is of importance to the business and industrial world; in the defense world, security concerns will dominate performance degradation.

WHAT HAVE WE LEARNED?

With the insights from the historical evolution of computer security and given the retrospective observations that can now be made, what specific things can now be said about things that have been learned?

- Interpretation of the concept of trust solely in terms of system software is too narrow.
- Trust and trustedness is a useful concept in many dimensions of computer security.
- We need to be able to measure, hopefully quantitatively, the level of trust of a component, of an overall system, of software, even of hardware.
- People must be included as one of the things whose level of trust must be evaluated and, ideally, measured.
- Nontechnical aspects of security (e.g., administrative, procedural) must be included in the trust evaluation for the overall system.

- There is much more to trusted systems than just technical measures.
- The public discussion of trust has been largely in the context of technical measures.
- The private sector, or even an individual community in it, does not "have its act together" in terms of specifying the threat, nor of identifying any special safeguards that will be needed beyond those now identified for the defense world.
- There are significant R&D efforts yet remaining.

  A foremost one is a set of security primitives from which macro-security controls can be constituted and function collectively as a trusted group. This will possibly become of more importance as the private sector understands its threat and security problems better. Another is the domestic/export issue.

WHAT CAN WE NOW SAY ABOUT TRUSTED SYSTEMS?

We can also make some specific assertions about trusted systems, the role of certified and evaluated products in them, and the influence of past history.

- Trusted systems can be implemented now.

  There is no need to wait for systems certified by some federal authority. Maybe the level of trustedness will not be ideal, especially the assurance measures may not be all that would be desired, but a significant level of trusted behavior can be achieved using what we now know how to do and installing the security safeguards that we now understand and can implement.
- In some, perhaps many cases, we will be pleasantly surprised to find that certified and evaluated systems or system components may not even be essential in private sector systems.

- There is no need to wait for trusted products; we can move out now.
- A trusted certified product or a trusted computing base does not assure a secure system, much less guarantee it.
- An organization can certainly get started right away on the part only it can do. An organization can build its own security safeguards into application programs; or if a large enough organization, can even make limited modifications to an operating system.

  There are dimensions that the end user will have to do anyway, so why wait? For example:

  Applications software
  Procedures
  Administrative and management overlay, etc.

- It must be understood that a certified system is not a magic bullet that, of itself, will be the answer to all security problems. It is one facet of a complex matter.
- As systems with some level of trust come into being, threat against them will mature and become more sophisticated; it will shift.

  Hence, the cat-and-mouse game must continue; security and trustedness will not be static attributes. On the contrary, both are likely to be rather dynamic.
- The level of trust must go up over time as the threat matures.
- The assurance issue will become more critical over time, because the threat against the safeguards per se will increase. In this regard, if one examines the assurance measures stipulated in the Orange Book, many of them are what would be called "good software engineering practices."

Design documentation
Formal specifications
Configuration management
Change control

No organization has a lock on such aspects of assurance. They are do-able by any organization that puts its software function--internal or contracted--in good order.

- While we do not have to wait for certified trusted products, neither is there harm in buying them now. The worst that can happen is unwarranted additional cost, and possibly an impact on performance.

THE BOTTOM LINE

The whole argument can now be pulled together. In outline form, it is the following.

- We are reasonably well convinced that we know how to do the security job in one community--defense. We have the vendor commitment to provide the necessary products.
- We have learned a lot about implementing technical security safeguards.
- We now better understand the political interplay between the security issue within government and the issue in the private sector.
- We have not yet learned very much about threat or appropriate safeguards against it in the various communities of the private sector.
- The vendor community has responded quite well "to the drummer" in the defense world. The private sector has yet to nominate or even find its drummer, and it is time that it does so.
- Given the status of things a short five to eight years ago, we now know a lot, but by no means do we know all. There is a long, long way to go in this thing we call computer security.

- There is a foundation of knowledge on which any organization can erect substantial deterrents against intrusions into its computer systems, and it can be done now.
- Certified evaluated systems will have their importance in the commercial community as the threat matures and becomes more sophisticated, and as the safeguards essential to counter that threat become technically more complex and more like those considered necessary in the defense communities.
- In the near future, the commercial private sector can do much for the security of its computer systems with present systems and present products.
- There is some homework to be done but it generally relates to a careful exposition of the threat, often by communities of common interest such as the savings bank industry or the retail department store industry, plus mutual agreement about the kinds and nature of safeguards that any one industry will need.

And, of course, the all important lesson for the private sector:

- Get organized and get the homework done so that practitioners of computer security can better help get safeguards in place.